



IFD

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Sandra E. Ring et al.  
Appl. No.: 10/789,460  
Filed: February 26, 2004  
Docket No.: 2037  
Conf. No. 5170  
Title: **METHODOLOGY, SYSTEM, COMPUTER READABLE  
MEDIUM, AND PRODUCT PROVIDING A SECURITY  
SOFTWARE SUITE FOR HANDLING OPERATING  
SYSTEM EXPLOITATIONS**

Art Unit: 2184  
Examiner:

Action: **TRANSMITTAL OF INFORMATION DISCLOSURE**  
Date: June 15, 2004

TO: Mail Stop DD  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Sir:

Pursuant to Applicants' duty of disclosure under 37 C.F.R. §1.56, Applicant is not aware of any specific prior art which relates to computer security systems, computer-readable media, security software products, or computerized methods, as disclosed and claimed in the above-identified patent application. The Examiner's attention, however, is directed to the background discussion in the application as it relates to known aspects of operating system exploitations, computer forensics and operating system recovery. Enclosed herewith is additional background information regarding the *Chkrootkit* and *Tripwire* rootkits that are referred to in the background section of the application.


Information has also come to the attention of the Applicant pertaining to security products available from Guidance Software, Inc., a company headquartered in Pasadena, California. The enclosed information was obtained

prior date of invention of the subject matter of the claims for the present application.

Accordingly, the identification of all of the above information is for the purpose of meeting Applicants' duty of disclosure under 37 C.F.R. Section 1.56 and is not intended to be an admission that any of this information constitutes prior art as to the invention disclosed and claimed in the subject application. Applicant, thus, believes that this application presents new, useful and non-obvious technology and that the claims presented with this application are allowable. The Examiner is courteously solicited to enter an expeditious allowance of this application. If any questions remain to be addressed, it is respectfully requested that the undersigned attorney for the Applicant be contacted at the number listed below.

Respectfully submitted,

***TIMOTHY J. MARTIN, P.C.***



---

Timothy J. Martin, #28,640  
Michael R. Henson, #39,222  
Rebecca A. Gegick, #51,724  
9250 W. 5th Avenue, Suite 200  
Lakewood, Colorado 80226  
(303) 232-3388

from the company's website at [www.guidancesoftware.com](http://www.guidancesoftware.com). More particularly, documentation is provided relating to at least two products referred to as the "EnCase Enterprise Edition" and the "EnCase Forensic Edition". Information is also provided pertaining to a component of at Enterprise Edition, referred to as the "EnCase Snapshot". According to material from the website, the "Snapshot" utility can be used manually or automatically to capture and preserve volatile data on servers and workstations, in an effort to identify anomalous activity as part of best practices for incidence response and computer forensic examinations.

It is not believed, however, that the Snapshot utility (or any other Guidance Software product for that matter) functions to locate a target memory range containing suspected data of interest, or actually search the short-term memory to locate such a target memory range. Moreover, Applicant also does not believe that these Guidance Software products are capable of copying data from volatile memory in a manner which avoids involving long-term memory resources, as contemplated and claimed in the present application.

It is believed that the enclosed information and associated products from Guidance Software were not publicly available prior to the Fall of 2003. Applicant notes that information pertaining to EnCase version 4.16 bears a November 2003 notice, and it is believed that white papers may have been available in about September 2003. As such, while it appears the availability of this information pre-dates Applicant's earliest filing date, it does not pre-date Applicant's date of invention and, should the need arise, Applicant is prepared to submit an appropriate oath or declaration under 37 C.F.R. §1.131 to establish a

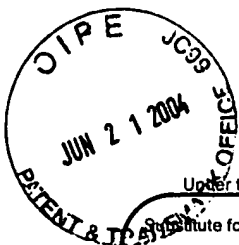


**CERTIFICATE OF MAILING UNDER 37 C.F.R. 1.8**

I hereby certify that the foregoing **TRANSMITTAL OF INFORMATION DISCLOSURE (4 pages) AND FORM PTO/SB/08 (1 page)** is being deposited with the United States Postal Service as first-class mail in an envelope addressed to Mail Stop DD, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 17<sup>th</sup> day of June, 2004.

Marcie F. King

Marcie F. King



PTO/SB/08B (08-03)

Approved for use through 07/31/2006. OMB 0651-0031  
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>  (Use as many sheets as necessary)				<b>Complete if Known</b>	
				Application Number	10/789,460
				Filing Date	February 26, 2004
				First Named Inventor	Sandra E. Ring et al
				Art Unit	2184
				Examiner Name	
Sheet	1	of	1	Attorney Docket Number	2037

NON PATENT LITERATURE DOCUMENTS			
Examiner Initials*	Cite No. <sup>1</sup>	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>
		"Tripwire's Website Materials" obtained from www.tripwire.org, Provided by Tripwire, Inc.	
		"chkrootkit's Website Materials" obtained from www.chkrootkit.com, Provided by chkrootkit.com	
		"Various Website Materials pertaining to EnCase Products" obtained from www.guidancesoftware.com, Provided by Guidance Software, Inc. 215 North Marengo Ave, 2nd Flr Pasadena, CA	

Examiner Signature	Date Considered
-----------------------	--------------------

\*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.